LILY HAY NEWMAN SECURITY 08.21.17 07:37 PM

A VERY DUMB MISTAKE COSTS CRYPTOCURRENCY INVESTORS BIG TIME

GETTY IMAGES

THE DIGITAL FINANCIAL services developer Enigma prides itself on ultra-secure products. The company's Catalyst platform protects financial info with a cutting-edge combination of blockchain-inspired privacy technology and cryptography. So it comes as no small surprise that on Monday, scammers took over the company's website, mailing lists, and Slack accounts by exploiting some extremely basic security mistakes Enigma had made. The blunders also

cryptocurrency fund-raising campaign that startups use when they want to raise capital for their company without going through the process of working with an established financial institution or venture capital fund. (The SEC has promised to clamp down on these ICOs, but so far is in the exploratory phase.)

RELATED STORIES

TOM SIMONITE
Regulators Warn Cryptocurrency Startup Fundraisers to Play By the Rules

GABRIEL NICHOLAS
Ethereum Is Coding's New Wild West

BRIAN BARRETT
Security News This Week: Two Huge Cryptocurrency Heists Cost Investors Millions

With the ICO in mind, scammers compromised official Enigma channels to create a sense of legitimacy and urgency. The plot proved easy to pull off. At least one of the passwords protecting the Enigma accounts, which included a Slack account with administrative privileges, had previously leaked, and reports indicate that the accounts weren't protected by two-factor authentication.

The hackers began defacing the company's main site and Slack accounts, and pushed a special "pre-sale" ahead of the ICO, directing money toward their own cryptocurrency wallet. They also went rogue on the company's mailing lists. Many users realized that the push was a scam, but the hustle did tempt some

called a crowd sale, was always set definitively for September 11, and emphasized that its secure servers had not been hacked. But a spokesperson confirmed that the scammers compromised account passwords using various methods. And in response to the incident, the company says it is adding strong, random passwords and two-factor authentication for each account, plus implementing robust password changing and better system compartmentalization. "We've moved up a number of critical security steps and taken additional measures to protect the community going forward," says Tor Bair, Enigma's head of marketing and growth. "We're now very well aware of the potential threats and are taking no chances."

Though honest mistakes can happen at any growing organization, the Enigma community grappled with the implications of the incident on Monday, wondering how a specialized cryptography company could only now be realizing the need for stringent account hygiene. "This will go down in crypto history as one of the stupidest moments ever. We need a meme," one Reddit user wrote. Some Redditors even claimed that they used the breached credential repository Have I Been Pwned to determine that the Enigma accounts scammers accessed reused a previously exposed account password from CEO Guy Zyskind. But Zyskind told WIRED that none of the breached Enigma accounts relied on reused passwords.

While the Enigma team worked to restore secure Slack service, the community's discussion moved to secure messaging app Telegram. "No word on honoring those who were scammed b/c of y'all negligence and poor security? Speaks volumes," a user called Jay wrote in the open chatroom. Many users indicated support for Enigma, though, and seemed satisfied with the company's remediation efforts.

the payment platform Viewpost. "To the public it looks as if the company has been hacked, and provides a significant amount of negative press about the company's security and privacy responsibilities."

Enigma said on Monday evening that it is working to mitigate the damage. "We're actively investigating the scam attempt and the parties involved with multiple partners, including vigilant members of our community, other companies in our space, and exchanges," Bair says.

Since they are unregulated by the government—for now, anyway—ICOs have perks that make them appealing to cryptocurrency companies, but by their nature they are also less predictable than standard fund-raising avenues. In mid July, scammers stole roughly $7 million from supporters during the ICO of the cryptocurrency management platform CoinDash. A few days later, hackers stole $32 million in Ethereum (though much of it was later recovered) by exploiting a vulnerability in a crypto product called Parity Wallet.

"The news of the attack is certainly not surprising," says Eric Klonowski, a senior advanced threat research analyst at the internet security firm Webroot. "Investors were ready to part with their money at a moment's notice, and the attacker was prepared to capitalize.... That said, recent core cryptocurrency heists are all a result of third-party vulnerabilities and their handling of investments, and not in the cryptography or implementation itself."

With the September 11 ICO still rapidly approaching, at least Enigma has some time to get its first-line security right.

#HACKS #CRYPTOCURRENCY #SECURITY

MORE SECURITY

TROLLS
Russian Propaganda Remains on Reddit
ISSIE LAPOWSKY

ESPIONAGE

'Slingshot' Spy Operation Used Routers to Hack Target PCs

ANDY GREENBERG

HANSA

Inside the Sting That Hijacked a Dark Web Drug Market

ANDY GREENBERG

AD BLOCKERS

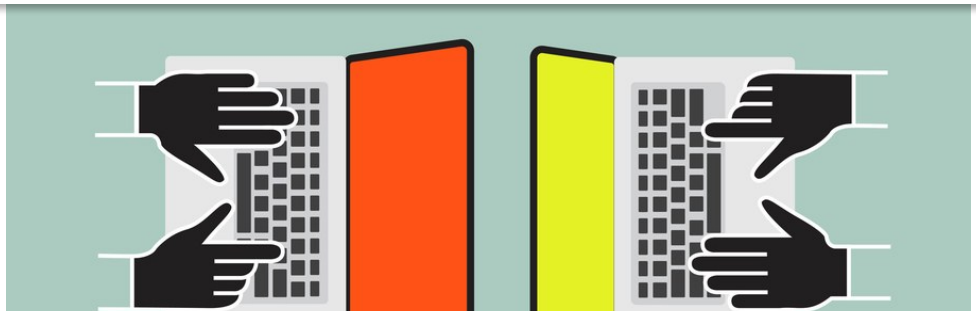
Ghostery Goes Open Source—And Has a New Business Model

LOUISE MATSAKIS

ETERNALBLUE

The Leaked NSA Spy Tool That Hacked the World

LILY HAY NEWMAN



CYBERATTACKS

Spy v. Spy: NSA Leak Reveals Agency's List of Enemy Hackers

ANDY GREENBERG